

Paros Scanning Report

Report generated at Wed, 8 Sep 2010 12:34:56.

Summary of Alerts

Risk Level	Number of Alerts
High	1
Medium	9
Low	3
Informational	0

Alert Detail

High (Warning) SQL Injection

Description SQL injection is possible. User parameters submitted will be formulated into a SQL query for database processing. If the query is built by simple 'string concatenation', it is possible to modify the meaning of the query by carefully crafting the parameters. Depending on the access right and type of database used, tampered query can be used to retrieve sensitive information from the database or execute arbitrary code. MS SQL and PostGreSQL, which supports multiple statements, may be exploited if the database access right is more powerful.

This can occur in URL query strings, POST paramters or even cookies. Currently check on cookie is not supported by Paros. You should check SQL injection manually as well as some blind SQL injection areas cannot be discovered by this check.

URL	https://hardening-mediawiki/index.php?title=MediaWiki:Common.css&usemsgcache=yes&ctype=text/css&smaxage=18000&action=raw&maxage=18000%20AND%201=1
Parameter	title=MediaWiki:Common.css&usemsgcache=yes&ctype=text/css&smaxage=18000&action=raw&maxage=18000 OR 1=1
URL	https://hardening-mediawiki/index.php?title=-&action=raw&smaxage=0%20AND%201=1&gen=js&useskin=monobook
Parameter	title=-&action=raw&smaxage=0 OR 1=1&gen=js&useskin=monobook
URL	https://hardening-mediawiki/index.php?title=-&action=raw&maxage=18000&smaxage=0%20AND%201=1&ts=20100907141908&gen=css
Parameter	title=-&action=raw&maxage=18000&smaxage=0 OR 1=1&ts=20100907141908&gen=css
URL	https://hardening-mediawiki/index.php?title=-&action=raw&maxage=18000&smaxage=0&ts=20100907141908%20AND%201=1&gen=css
Parameter	title=-&action=raw&maxage=18000&smaxage=0&ts=20100907141908 OR 1=1&gen=css
URL	https://hardening-mediawiki/index.php?title=-&action=raw&maxage=18000%20AND%201=1&smaxage=0&ts=20100907141908&gen=css

Parameter	title=-&action=raw&maxage=18000 OR 1=1&smaxage=0&ts=20100907141908&gen=css
URL	https://hardening-mediawiki/index.php?title=MediaWiki:Common.css&usemsgcache=yes&ctype=text/css&smaxage=18000%20AND%201=1&action=raw&maxage=18000
Parameter	title=MediaWiki:Common.css&usemsgcache=yes&ctype=text/css&smaxage=18000 OR 1=1&action=raw&maxage=18000
URL	https://hardening-mediawiki/index.php?title=MediaWiki:Common.css&usemsgcache=yes&ctype=text/css%20AND%201=1&smaxage=18000&action=raw&maxage=18000
Parameter	title=MediaWiki:Common.css&usemsgcache=yes&ctype=text/css OR 1=1&smaxage=18000&action=raw&maxage=18000
Solution	<p>Do not trust client side input even if there is client side validation. In general,</p> <ul style="list-style-type: none"> • If the input string is numeric, type check it. • If the application used JDBC, use PreparedStatement or CallableStatement with parameters passed by '?' • If the application used ASP, use ADO Command Objects with strong type checking and parameterized query. • If stored procedure or bind variables can be used, use it for parameter passing into query. Do not just concatenate string into query in the stored procedure! • Do not create dynamic SQL query by simple string concatenation. • Use minimum database user privilege for the application. This does not eliminate SQL injection but minimize its damage. Eg if the application require reading one table only, grant such access to the application. Avoid using 'sa' or 'db-owner'.
Reference	<ul style="list-style-type: none"> • The OWASP guide at http://www.owasp.org/documentation/guide • http://www.sqlsecurity.com/DesktopDefault.aspx?tabid=23 • http://www.spidynamics.com/whitepapers/WhitepaperSQLInjection.pdf • For Oracle database, refer to http://www.integrigy.com/info/IntegrigyIntrotoSQLInjectionAttacks.pdf

Medium (Warning) Directory browsing

Description	It is possible to view the directory listing. Directory listing may reveal hidden scripts, include files , backup source files etc which be accessed to read sensitive information.
URL	https://hardening-mediawiki/skins/common/images/de/
URL	https://hardening-mediawiki/skins/monobook/
URL	https://hardening-mediawiki/skins/common/
URL	https://hardening-mediawiki/skins/common/images/
URL	https://hardening-mediawiki/skins/

URL	https://hardening-mediawiki/skins/chick/
URL	https://hardening-mediawiki/images/b/b3/
URL	https://hardening-mediawiki/images/
URL	https://hardening-mediawiki/extensions/SemanticMediaWiki/skins/images/
URL	https://hardening-mediawiki/images/b/
URL	https://hardening-mediawiki/extensions/SemanticMediaWiki/
URL	https://hardening-mediawiki/extensions/SemanticMediaWiki/skins/
URL	https://hardening-mediawiki/extensions/PhpIds/extjs/resources/css/
URL	https://hardening-mediawiki/extensions/PhpIds/extjs/resources/
URL	https://hardening-mediawiki/extensions/PhpIds/extjs/examples/shared/
URL	https://hardening-mediawiki/extensions/PhpIds/extjs/pie-chart/
URL	https://hardening-mediawiki/extensions/PhpIds/extjs/adapters/ext/
URL	https://hardening-mediawiki/extensions/PhpIds/extjs/examples/
URL	https://hardening-mediawiki/extensions/PhpIds/extjs/
URL	https://hardening-mediawiki/extensions/PhpIds/extjs/adapters/
URL	https://hardening-mediawiki/extensions/PhpIds/Layout/
URL	https://hardening-mediawiki/extensions/PhpIds/
URL	https://hardening-mediawiki/extensions/
URL	https://hardening-mediawiki/extensions/CategoryTree/

Solution	Disable directory browsing. If this is required, make sure the listed files does not induce risks.
----------	--

Reference	For IIS, turn off directory browsing.
-----------	---------------------------------------

For Apache, use the 'Options -Indexes' directive to disable indexes in directory or via .htaccess:

- . <http://httpd.apache.org/docs/mod/core.html#options>
- . <http://alamo.satlug.org/pipermail/satlug/2002-February/000053.html>
- . or create a default index.html for each directory.

Medium (Warning) Secure page browser cache

Description	Secure page can be cached in browser. Cache control is not set in HTTP header nor HTML header. Sensitive content can be recovered from browser storage.
URL	https://hardening-mediawiki/skins/monobook/common.css
URL	https://hardening-mediawiki/skins/monobook/main.css?207
URL	https://hardening-mediawiki/skins/common/shared.css?207
URL	https://hardening-mediawiki/skins/common/wikibits.js?207
URL	https://hardening-mediawiki/skins/common/edit.js?207
URL	https://hardening-mediawiki/skins/common/history.js?207
URL	https://hardening-mediawiki/skins/common/block.js?207
URL	https://hardening-mediawiki/skins/common/commonPrint.css?207
URL	https://hardening-mediawiki/skins/common/ajax.js?207
URL	https://hardening-mediawiki/skins/common/ajaxwatch.js?207
URL	https://hardening-mediawiki/index.php/Spezial:Browse/Semantisches_eStudy_Wiki
URL	https://hardening-mediawiki/skins/chick/?207
URL	https://hardening-mediawiki/index.php/Spezial:Sperren
URL	https://hardening-mediawiki/index.php/Spezial:Spezialseiten
URL	https://hardening-mediawiki/index.php/Spezial:PHPIDSadmin

URL <https://hardening-mediawiki/index.php/Spezial:PHPIDSadmin?select=Stats&action=menu>

URL <https://hardening-mediawiki/index.php/Hauptseite>

URL https://hardening-mediawiki/index.php/Spezial:Liste_der_Sperren

URL https://hardening-mediawiki/extensions/SemanticMediaWiki/skins/SMW_custom.css?207

URL https://hardening-mediawiki/extensions/SemanticMediaWiki/skins/SMW_tooltip.js

URL <https://hardening-mediawiki/extensions/PhpIds/extjs/pie-chart/pie-chart.js>

URL <https://hardening-mediawiki/extensions/PhpIds/extjs/resources/css/ext-all.css>

URL <https://hardening-mediawiki/extensions/PhpIds/extjs/adaptor/ext/ext-base.js>

URL <https://hardening-mediawiki/extensions/PhpIds/extjs/examples/shared/examples.js>

URL <https://hardening-mediawiki/extensions/CategoryTree/CategoryTree.js?5>

URL <https://hardening-mediawiki/extensions/PhpIds/extjs/ext-all.js>

URL https://hardening-mediawiki/index.php?title=Semantisches_eStudy_Wiki&action=submit

URL <https://hardening-mediawiki/extensions/CategoryTree/CategoryTree.css?5>

URL <https://hardening-mediawiki/index.php?title=-&action=raw&smaxage=0&gen=js&useskin=monobook>

URL https://hardening-mediawiki/index.php?title=Semantisches_eStudy_Wiki&action=history

URL <https://hardening-mediawiki/index.php?title=MediaWiki:Common.css&usemsgcache=yes&ctype=text%2Fcss&smaxage=18000&action=raw&maxage=18000>

URL <https://hardening-mediawiki/index.php?title=-&action=raw&maxage=18000&smaxage=0&ts=20100907141908&gen=css>

Solution The best way is to set HTTP header with: 'Pragma: No-cache' and 'Cache-control: No-cache'.

Alternatively, this can be set in the HTML header by:

```
<META HTTP-EQUIV='Pragma' CONTENT='no-cache'>
```

```
<META HTTP-EQUIV='Cache-Control' CONTENT='no-cache'>
```

but some browsers may have problem using this method.

Reference . How to prevent caching in Internet Explorer - <http://support.microsoft.com/default.aspx?kbid=234067>

. Pragma: No-cache Tag May Not Prevent Page from Being Cached - <http://support.microsoft.com/default.aspx?kbid=222064>

**Medium
(Suspicious)**

IIS default file

Description	Microsoft IIS 4.0, 5.0 or 6.0 default files are found.
URL	https://hardening-mediawiki/iisstart.htm
URL	https://hardening-mediawiki/samples/sampsite/taste.htm
URL	https://hardening-mediawiki/samples/sampsite/sendme.htm
URL	https://hardening-mediawiki/samples/sampsite/sampsite.htm
URL	https://hardening-mediawiki/samples/sampsite/results.htm
URL	https://hardening-mediawiki/samples/sampsite/process.htm
URL	https://hardening-mediawiki/samples/sampsite/default.htm
URL	https://hardening-mediawiki/samples/sampsite/catalog.htm
URL	https://hardening-mediawiki/samples/sampsite/about.htm
URL	https://hardening-mediawiki/samples/isapi/srch.htm
URL	https://hardening-mediawiki/samples/isapi/isapi.htm
URL	https://hardening-mediawiki/samples/isapi/favlist.htm
URL	https://hardening-mediawiki/samples/isapi/drop.htm
URL	https://hardening-mediawiki/samples/htmlsamp/tables.htm
URL	https://hardening-mediawiki/samples/htmlsamp/styles2.htm
URL	https://hardening-mediawiki/samples/htmlsamp/styles.htm

URL	https://hardening-mediawiki/samples/htmlsamp/htmlsamp.htm
URL	https://hardening-mediawiki/samples/gbook/register.htm
URL	https://hardening-mediawiki/samples/gbook/query.htm
URL	https://hardening-mediawiki/samples/dbsamp/dbsamp3.htm
URL	https://hardening-mediawiki/samples/dbsamp/dbsamp2.htm
URL	https://hardening-mediawiki/samples/dbsamp/dbsamp1.htm
URL	https://hardening-mediawiki/samples/dbsamp/dbsamp.htm
URL	https://hardening-mediawiki/msadc/readme.txt
URL	https://hardening-mediawiki/msadc/msadcs.dll
URL	https://hardening-mediawiki/msadc/adcvbs.inc
URL	https://hardening-mediawiki/msadc/adccvbs.inc
URL	https://hardening-mediawiki/iisadmpwd/annot3.htm
URL	https://hardening-mediawiki/iisadmpwd/annot.htm
URL	https://hardening-mediawiki/iisadmpwd/aexp4b.htm
URL	https://hardening-mediawiki/iisadmpwd/aexp4.htm
URL	https://hardening-mediawiki/iisadmpwd/aexp3.htm
URL	https://hardening-mediawiki/iisadmpwd/aexp2b.htm
URL	https://hardening-mediawiki/iisadmpwd/aexp2.htm
URL	https://hardening-mediawiki/iisadmpwd/aexp.htm
URL	https://hardening-mediawiki/iisadmpwd/achg.htm
URL	https://hardening-mediawiki/scripts/tools/newdsn.exe
URL	https://hardening-mediawiki/scripts/tools/mkilog.exe

URL	https://hardening-mediawiki/scripts/tools/getdrvrs.exe
URL	https://hardening-mediawiki/scripts/tools/dsnform.exe
URL	https://hardening-mediawiki/iisadmin/htmldocs/iisdocs.htm
URL	https://hardening-mediawiki/iissamples/ExAir/About.asp
URL	https://hardening-mediawiki/iissamples/ExAir/HowToReachUs.asp
URL	https://hardening-mediawiki/iissamples/ExAir/FunNGames/FunNGames.asp
URL	https://hardening-mediawiki/iissamples/ExAir/Catalog/Catalog.asp
URL	https://hardening-mediawiki/iissamples/ExAir/IEPush/Channel.asp
URL	https://hardening-mediawiki/iissamples/ExAir/default.asp
URL	https://hardening-mediawiki/iissamples/default/samples.asp
URL	https://hardening-mediawiki/_vti_cnf/
URL	https://hardening-mediawiki/_vti_txt/
URL	https://hardening-mediawiki/_vti_log/
URL	https://hardening-mediawiki/_vti_pvt/
URL	https://hardening-mediawiki/_vti_bin/
URL	https://hardening-mediawiki/_private/
URL	https://hardening-mediawiki/msadc/samples/adctest.asp
URL	https://hardening-mediawiki/msadc/samples/selector/showcode.asp
URL	https://hardening-mediawiki/IISamples/sdk/asp/database/Update_VBScript.asp
URL	https://hardening-mediawiki/IISamples/sdk/asp/database/StoredProcedures_VBScript.asp
URL	https://hardening-mediawiki/IISamples/sdk/asp/database/SimpleQuery_VBScript.asp
URL	https://hardening-mediawiki/IISamples/sdk/asp/database/MultiScrolling_VBScript.asp

URL	https://hardening-mediawiki/IISamples/sdk/asp/database/LimitRows_VBScript.asp
URL	https://hardening-mediawiki/IISamples/sdk/asp/database/AddDelete_VBScript.asp
URL	https://hardening-mediawiki/IISamples/sdk/asp/applications/Session_VBScript.asp
URL	https://hardening-mediawiki/IISamples/sdk/asp/applications/Session_JScript.asp
URL	https://hardening-mediawiki/IISamples/sdk/asp/applications/Application_VBScript.asp
URL	https://hardening-mediawiki/IISamples/sdk/asp/applications/Application_JScript.asp
URL	https://hardening-mediawiki/IISamples/sdk/asp/docs/toolbar.asp
URL	https://hardening-mediawiki/IISamples/sdk/asp/docs/sampfram.asp
URL	https://hardening-mediawiki/IISamples/sdk/asp/docs/libcodebrws.inc
URL	https://hardening-mediawiki/IISamples/sdk/asp/docs/ColorPicker.asp
URL	https://hardening-mediawiki/IISamples/sdk/asp/docs/CodeBrws.asp
URL	https://hardening-mediawiki/vti_txt/
URL	https://hardening-mediawiki/_vti_script/
URL	https://hardening-mediawiki/_vti_pvt/
URL	https://hardening-mediawiki/_vti_log/
URL	https://hardening-mediawiki/_vti_cnf/
URL	https://hardening-mediawiki/_private/
URL	https://hardening-mediawiki/_vti_bin/
URL	https://hardening-mediawiki/_cti_pvt/writeto.cnf
URL	https://hardening-mediawiki/_cti_pvt/uniqperm.cnf
URL	https://hardening-mediawiki/_cti_pvt/svcacl.cnf
URL	https://hardening-mediawiki/_cti_pvt/services.cnf

URL	https://hardening-mediawiki/_cti_pvt/service.cnf
URL	https://hardening-mediawiki/_cti_pvt/linkinfo.cnf
URL	https://hardening-mediawiki/_cti_pvt/dectodep.btr
URL	https://hardening-mediawiki/_cti_pvt/deptodoc.btr
URL	https://hardening-mediawiki/_cti_pvt/bots.cnf
URL	https://hardening-mediawiki/_cti_pvt/botinfo.cnf
URL	https://hardening-mediawiki/_cti_pvt/access.cnf
URL	https://hardening-mediawiki/_vti_bin/_vti_aut/author.dll
URL	https://hardening-mediawiki/_vti_bin/_vti_adm/admin.dll
URL	https://hardening-mediawiki/_vti_bin/shtml.dll
URL	https://hardening-mediawiki/_vti_bin/fpcount.exe
URL	https://hardening-mediawiki/msadc/msadcs.dll
URL	https://hardening-mediawiki/_vti_inf.html
URL	https://hardening-mediawiki/postinfo.html
URL	https://hardening-mediawiki/iisstart.asp

Solution Remove default files and virtual directories.

Reference

**Medium
(Suspicious)**

Cold Fusion default file

Description ColdFusion MX default files are found.

URL <https://hardening-mediawiki/CFIDE/administrator/welcomegetstart.cfm>

URL <https://hardening-mediawiki/CFIDE/administrator/welcomefooter.cfm>

URL	https://hardening-mediawiki/CFIDE/administrator/welcomeexapps.cfm
URL	https://hardening-mediawiki/CFIDE/administrator/welcomedoc.cfm
URL	https://hardening-mediawiki/CFIDE/administrator/welcome.cfm
URL	https://hardening-mediawiki/CFIDE/administrator/tabs.cfm
URL	https://hardening-mediawiki/CFIDE/administrator/right.cfm
URL	https://hardening-mediawiki/CFIDE/administrator/navserver.cfm
URL	https://hardening-mediawiki/CFIDE/administrator/logout.cfm
URL	https://hardening-mediawiki/CFIDE/administrator/login.cfm
URL	https://hardening-mediawiki/CFIDE/administrator/linkdirect.cfm
URL	https://hardening-mediawiki/CFIDE/administrator/left.cfm
URL	https://hardening-mediawiki/CFIDE/administrator/index.cfm
URL	https://hardening-mediawiki/CFIDE/administrator/homepage.cfm
URL	https://hardening-mediawiki/CFIDE/administrator/homefile.cfm
URL	https://hardening-mediawiki/CFIDE/administrator/header.cfm
URL	https://hardening-mediawiki/CFIDE/administrator/enter.cfm
URL	https://hardening-mediawiki/CFIDE/administrator/checkfile.cfm
URL	https://hardening-mediawiki/CFIDE/administrator/Application.cfm
URL	https://hardening-mediawiki/CFIDE/administrator/aboutcf.cfm

Solution Remove default files.

Reference

Medium (Suspicious) Macromedia JRun default files

Description	JRun 4.0 default files are found or application information disclosure.
URL	https://hardening-mediawiki/databasenotes.html
URL	https://hardening-mediawiki/SmarTicketApp/index.html
URL	https://hardening-mediawiki/flash/java/javabean/FlashJavaBean.html
URL	https://hardening-mediawiki/ws-client/loanCalculation.jsp
URL	https://hardening-mediawiki/techniques/servlets/index.html
URL	https://hardening-mediawiki/worldmusic/action/catalog
URL	https://hardening-mediawiki/worldmusic/action/cdlist
URL	https://hardening-mediawiki/travelnet/home.jsp
URL	https://hardening-mediawiki/compass/logon.jsp
URL	https://hardening-mediawiki/jstl-war/index.html
URL	https://hardening-mediawiki/WEB-INF/webapp.properties
URL	https://hardening-mediawiki/WEB-INF/web.xml

Solution Remove default files.

Reference

**Medium
(Suspicious)** **Tomcat source file disclosure**

Description Tomcat source file disclosed.

URL <https://hardening-mediawiki/.jsp>

Solution Upgrade to newer version.

Reference

Medium (Suspicious)	BEA WebLogic example files
Description	BEA WebLogic server 8.1 example files are found
URL	https://hardening-mediawiki/wliconsole
URL	https://hardening-mediawiki/portalAppAdmin/login.jsp
URL	https://hardening-mediawiki/e2ePortalProject/Login.portal
URL	https://hardening-mediawiki/examplesWebApp/SessionServlet
URL	https://hardening-mediawiki/examplesWebApp/InteractiveQuery.jsp
URL	https://hardening-mediawiki/examplesWebApp/EJBBeanManagedClient.jsp
URL	https://hardening-mediawiki/examplesWebApp/WebservicesEJB.jsp
URL	https://hardening-mediawiki/examplesWebApp/OrderParser.jsp?xmlfile=C:/bea/weblogic81/samples/server/examples/src/examples/xml/orderParser/order.xml
URL	https://hardening-mediawiki/examplesWebApp/index.jsp
URL	https://hardening-mediawiki/physican/login.do
URL	https://hardening-mediawiki/admin/login.do
URL	https://hardening-mediawiki/patient/login.do
URL	https://hardening-mediawiki/patient/register.do
Solution	Remove example files.
Reference	

Medium (Suspicious)	IBM WebSphere default files
Description	IBM WebSphere 4.0/5.0 example files are found.
URL	https://hardening-mediawiki/IBMWebAS
URL	https://hardening-mediawiki/theme

URL	https://hardening-mediawiki/estore/populate
URL	https://hardening-mediawiki/estore/annotated-index.html
URL	https://hardening-mediawiki/estore/index.html
URL	https://hardening-mediawiki/WebSphereSamples/
URL	https://hardening-mediawiki/WebSphereSamples/SingleSamples/AccountAndTransfer/create.html
URL	https://hardening-mediawiki/WebSphereSamples/SingleSamples/Increment/increment.html
URL	https://hardening-mediawiki/WebSphereSamples/YourCo/main.html
URL	https://hardening-mediawiki/WebSphereSamples/
URL	https://hardening-mediawiki/webapp/examples/HelloPervasive
URL	https://hardening-mediawiki/webapp/examples/verify
URL	https://hardening-mediawiki/webapp/examples/HitCount
URL	https://hardening-mediawiki/webapp/examples/showcfg
URL	https://hardening-mediawiki/webapp/examples/ping
URL	https://hardening-mediawiki/webapp/examples/ErrorHandler
URL	https://hardening-mediawiki/webapp/examples/simple.jsp
URL	https://hardening-mediawiki/webapp/examples/login.html
URL	https://hardening-mediawiki/servlet/ErrorHandler
URL	https://hardening-mediawiki/servlet/hello
URL	https://hardening-mediawiki/servlet/SnoopServlet
URL	https://hardening-mediawiki/servlet/snoop2
URL	https://hardening-mediawiki/servlet/snoop
URL	https://hardening-mediawiki/admin/secure/logon.jsp

URL	https://hardening-mediawiki/admin/logon.jsp
URL	https://hardening-mediawiki/webapp/examples/HitCount
URL	https://hardening-mediawiki/servlet/aphtpassword
URL	https://hardening-mediawiki/servlet/SimpleServlet
URL	https://hardening-mediawiki/servlet/HelloWorldServlet

Solution Remove example files.

Reference

Medium (Suspicious) Lotus Domino default files

Description Lotus Domino default files found.

URL	https://hardening-mediawiki/userreg.nsf
URL	https://hardening-mediawiki/smvlog.nsf
URL	https://hardening-mediawiki/streg.nsf
URL	https://hardening-mediawiki/smtp.box
URL	https://hardening-mediawiki/smtp.nsf
URL	https://hardening-mediawiki/smtpibwq.nsf
URL	https://hardening-mediawiki/smtpobwq.nsf
URL	https://hardening-mediawiki/smsolar.nsf
URL	https://hardening-mediawiki/smtime.nsf
URL	https://hardening-mediawiki/smmsg.nsf
URL	https://hardening-mediawiki/smquar.nsf
URL	https://hardening-mediawiki/smency.nsf

URL	https://hardening-mediawiki/smhelp.nsf
URL	https://hardening-mediawiki/sample/siregw46.nsf
URL	https://hardening-mediawiki/smconf.nsf
URL	https://hardening-mediawiki/qpadmin.nsf
URL	https://hardening-mediawiki/quickplace/quickplace/main.nsf
URL	https://hardening-mediawiki/nntp/nd000002.nsf
URL	https://hardening-mediawiki/nntp/nd000003.nsf
URL	https://hardening-mediawiki/mtstore.nsf
URL	https://hardening-mediawiki/nntp/nd000001.nsf
URL	https://hardening-mediawiki/mail9.box
URL	https://hardening-mediawiki/msdwda.nsf
URL	https://hardening-mediawiki/mail7.box
URL	https://hardening-mediawiki/mail8.box
URL	https://hardening-mediawiki/mail5.box
URL	https://hardening-mediawiki/mail6.box
URL	https://hardening-mediawiki/mail3.box
URL	https://hardening-mediawiki/mail4.box
URL	https://hardening-mediawiki/mail1.box
URL	https://hardening-mediawiki/mail2.box
URL	https://hardening-mediawiki/l_domlog.nsf
URL	https://hardening-mediawiki/mail10.box
URL	https://hardening-mediawiki/leilog.nsf

URL	https://hardening-mediawiki/leivlt.nsf
URL	https://hardening-mediawiki/jotter.nsf
URL	https://hardening-mediawiki/leiadm.nsf
URL	https://hardening-mediawiki/domlog.nsf
URL	https://hardening-mediawiki/iNotes/Forms5.nsf/\$DefaultNav
URL	https://hardening-mediawiki/dirassist.nsf
URL	https://hardening-mediawiki/doladmin.nsf
URL	https://hardening-mediawiki/decslog.nsf
URL	https://hardening-mediawiki/DEESAdmin.nsf
URL	https://hardening-mediawiki/DEASLog05.nsf
URL	https://hardening-mediawiki/DEASLog.nsf
URL	https://hardening-mediawiki/DEASLog03.nsf
URL	https://hardening-mediawiki/DEASLog04.nsf
URL	https://hardening-mediawiki/DEASLog01.nsf
URL	https://hardening-mediawiki/DEASLog02.nsf
URL	https://hardening-mediawiki/da.nsf
URL	https://hardening-mediawiki/DEASAppDesign.nsf
URL	https://hardening-mediawiki/clbdbdir.nsf
URL	https://hardening-mediawiki/clusta4.nsf
URL	https://hardening-mediawiki/bookmark.nsf
URL	https://hardening-mediawiki/clbusy.nsf
URL	https://hardening-mediawiki/852566C90012664F

URL	https://hardening-mediawiki/a_domlog.nsf
URL	https://hardening-mediawiki/vpuserinfo.nsf
URL	https://hardening-mediawiki/web.nsf
URL	https://hardening-mediawiki/stlog.nsf
URL	https://hardening-mediawiki/stsrc.nsf
URL	https://hardening-mediawiki/stdnaset.nsf
URL	https://hardening-mediawiki/stdomino.nsf
URL	https://hardening-mediawiki/stconfig.nsf
URL	https://hardening-mediawiki/stconf.nsf
URL	https://hardening-mediawiki/stauths.nsf
URL	https://hardening-mediawiki/stautht.nsf
URL	https://hardening-mediawiki/srvnam.htm
URL	https://hardening-mediawiki/statrep.nsf
URL	https://hardening-mediawiki/setup.nsf
URL	https://hardening-mediawiki/smbcfg.nsf
URL	https://hardening-mediawiki/schema50.nsf
URL	https://hardening-mediawiki/setupweb.nsf
URL	https://hardening-mediawiki/perweb.nsf
URL	https://hardening-mediawiki/quickplacequickplacemain.nsf
URL	https://hardening-mediawiki/nntppost.nsf
URL	https://hardening-mediawiki/ntsync45.nsf
URL	https://hardening-mediawiki/log4a.nsf

URL	https://hardening-mediawiki/mab.nsf
URL	https://hardening-mediawiki/events.nsf
URL	https://hardening-mediawiki/event.nsf
URL	https://hardening-mediawiki/domguide.nsf
URL	https://hardening-mediawiki/events5.nsf
URL	https://hardening-mediawiki/domadmin.nsf
URL	https://hardening-mediawiki/domcfg.nsf
URL	https://hardening-mediawiki/deslog.nsf
URL	https://hardening-mediawiki/domadmin.nsf
URL	https://hardening-mediawiki/dclf.nsf
URL	https://hardening-mediawiki/decsadm.nsf
URL	https://hardening-mediawiki/collect4.nsf
URL	https://hardening-mediawiki/dba4.nsf
URL	https://hardening-mediawiki/chatlog.nsf
URL	https://hardening-mediawiki/certlog.nsf
URL	https://hardening-mediawiki/certa.nsf
URL	https://hardening-mediawiki/bookmarks.nsf
URL	https://hardening-mediawiki/alog.nsf
URL	https://hardening-mediawiki/admin.nsf
URL	https://hardening-mediawiki/admin5.nsf
URL	https://hardening-mediawiki/?Open
URL	https://hardening-mediawiki/?OpenServer

URL	https://hardening-mediawiki/webadmin.nsf
URL	https://hardening-mediawiki/statmail.nsf
URL	https://hardening-mediawiki/reports.nsf
URL	https://hardening-mediawiki/names.nsf
URL	https://hardening-mediawiki/mtatbls.nsf
URL	https://hardening-mediawiki/mail.box
URL	https://hardening-mediawiki/log.nsf
URL	https://hardening-mediawiki/events4.nsf
URL	https://hardening-mediawiki/dspug.nsf
URL	https://hardening-mediawiki/certsrv.nsf
URL	https://hardening-mediawiki/catalog.nsf
URL	https://hardening-mediawiki/busytime.nsf
URL	https://hardening-mediawiki/agentrunner.nsf
URL	https://hardening-mediawiki/admin4.nsf
URL	https://hardening-mediawiki/homepage.nsf

Solution Remove default files.

Reference

Low (Warning) Obsolete file

Description	Miscellaneous include files, backup, unused or obsolete files exist as indicated. If these files contain program source, information such as server logic or ODBC/JDBC user ID and passwords may be revealed since these file extension may not be processed by the web server.
URL	https://hardening-mediawiki/skins.inc

URL	https://hardening-mediawiki/skins~
URL	https://hardening-mediawiki/skins.bak
URL	https://hardening-mediawiki/skins.inc
URL	https://hardening-mediawiki/skins.old
URL	https://hardening-mediawiki/skins.bak
URL	https://hardening-mediawiki/index.php/Spezial:Browse/Semantisches_eStudy_Wiki~
URL	https://hardening-mediawiki/skins.old
URL	https://hardening-mediawiki/index.php/Spezial:Browse/Semantisches_eStudy_Wiki.inc
URL	https://hardening-mediawiki/index.inc
URL	https://hardening-mediawiki/index.bak
URL	https://hardening-mediawiki/index.inc
URL	https://hardening-mediawiki/index.bak
URL	https://hardening-mediawiki/index.php/Spezial:Browse/Semantisches_eStudy_Wiki.bak
URL	https://hardening-mediawiki/index.php/Spezial:Browse/Semantisches_eStudy_Wiki.old
URL	https://hardening-mediawiki/index.old
URL	https://hardening-mediawiki/index.inc
URL	https://hardening-mediawiki/index.old
URL	https://hardening-mediawiki/index.inc
URL	https://hardening-mediawiki/index.bak
URL	https://hardening-mediawiki/index.bak
URL	https://hardening-mediawiki/index.old
URL	https://hardening-mediawiki/index.inc?select=Stats&action=menu

URL	https://hardening-mediawiki/index.old
URL	https://hardening-mediawiki/index.inc
URL	https://hardening-mediawiki/index.bak?select=Stats&action=menu
URL	https://hardening-mediawiki/index.bak
URL	https://hardening-mediawiki/index.old?select=Stats&action=menu
URL	https://hardening-mediawiki/index.old
URL	https://hardening-mediawiki/index.inc
URL	https://hardening-mediawiki/index.old
URL	https://hardening-mediawiki/index.bak
URL	https://hardening-mediawiki/index.bak
URL	https://hardening-mediawiki/index.inc
URL	https://hardening-mediawiki/index.old
URL	https://hardening-mediawiki/index.inc
URL	https://hardening-mediawiki/images~
URL	https://hardening-mediawiki/index.bak
URL	https://hardening-mediawiki/images.inc
URL	https://hardening-mediawiki/index.old
URL	https://hardening-mediawiki/images.inc
URL	https://hardening-mediawiki/index.inc
URL	https://hardening-mediawiki/images.bak
URL	https://hardening-mediawiki/index.bak
URL	https://hardening-mediawiki/images.bak

URL	https://hardening-mediawiki/index.old
URL	https://hardening-mediawiki/extensions~
URL	https://hardening-mediawiki/images.old
URL	https://hardening-mediawiki/extensions.inc
URL	https://hardening-mediawiki/images.old
URL	https://hardening-mediawiki/extensions.bak
URL	https://hardening-mediawiki/extensions.inc
URL	https://hardening-mediawiki/extensions.old
URL	https://hardening-mediawiki/extensions.bak
URL	https://hardening-mediawiki/extensions.old
URL	https://hardening-mediawiki/index.inc?title=Semantisches_eStudy_Wiki&action=submit
URL	https://hardening-mediawiki/index.inc?title=Semantisches_eStudy_Wiki&action=submit
URL	https://hardening-mediawiki/index.bak?title=Semantisches_eStudy_Wiki&action=submit
URL	https://hardening-mediawiki/index.bak?title=Semantisches_eStudy_Wiki&action=submit
URL	https://hardening-mediawiki/index.old?title=Semantisches_eStudy_Wiki&action=submit
URL	https://hardening-mediawiki/index.inc?title=Semantisches_eStudy_Wiki&action=history
URL	https://hardening-mediawiki/index.old?title=Semantisches_eStudy_Wiki&action=submit
URL	https://hardening-mediawiki/index.old?title=Semantisches_eStudy_Wiki&action=history
URL	https://hardening-mediawiki/index.bak?title=Semantisches_eStudy_Wiki&action=history

Solution Remove backup, unused or obsolete files. For include files, carefully choose the suffix to prevent information disclosure.

Reference

Low (Warning)

Private IP disclosure

Description	Private IP such as 10.x.x.x, 172.x.x.x, 192.168.x.x is found in the HTTP response body. This can be used in exploits on internal system.
URL	https://hardening-mediawiki/index.php/Spezial:Liste_der_Sperren
Other information	10.20.0.93
URL	https://hardening-mediawiki/index.php/Spezial:Liste_der_Sperren
Other information	10.20.0.93
URL	https://hardening-mediawiki/index.php/Spezial:Liste_der_Sperren
Other information	10.20.0.93
URL	https://hardening-mediawiki/index.php/Spezial:Liste_der_Sperren
Other information	10.20.0.93
URL	https://hardening-mediawiki/index.php/Spezial:Liste_der_Sperren
Other information	10.20.0.93
URL	https://hardening-mediawiki/index.php/Spezial:Liste_der_Sperren
Other information	10.20.0.93
URL	https://hardening-mediawiki/index.php/Spezial:Liste_der_Sperren
Other information	10.20.0.93
URL	https://hardening-mediawiki/index.php/Spezial:Liste_der_Sperren
Other information	10.20.0.93
URL	https://hardening-mediawiki/index.php/Spezial:Liste_der_Sperren

Other information	10.20.0.93
URL	https://hardening-mediawiki/index.php/Spezial:Liste_der_Sperren
Other information	10.20.0.93
URL	https://hardening-mediawiki/index.php/Spezial:Liste_der_Sperren
Other information	10.20.0.93
URL	https://hardening-mediawiki/index.php/Spezial:Liste_der_Sperren
Other information	10.20.0.93
URL	https://hardening-mediawiki/index.php/Spezial:Liste_der_Sperren
Other information	10.20.0.93
URL	https://hardening-mediawiki/index.php/Spezial:Liste_der_Sperren
Other information	10.20.0.93
URL	https://hardening-mediawiki/index.php/Spezial:Liste_der_Sperren
Other information	10.192.5.247
URL	https://hardening-mediawiki/index.php/Spezial:Liste_der_Sperren
Other information	10.192.5.247
URL	https://hardening-mediawiki/index.php/Spezial:Liste_der_Sperren
Other information	10.192.5.247
URL	https://hardening-mediawiki/index.php/Spezial:Liste_der_Sperren
Other information	10.192.5.247

URL	https://hardening-mediawiki/index.php/Spezial:Liste_der_Sperren
Other information	10.192.5.247
URL	https://hardening-mediawiki/index.php/Spezial:Liste_der_Sperren
Other information	10.192.5.247
URL	https://hardening-mediawiki/index.php/Spezial:Liste_der_Sperren
Other information	10.192.5.247
URL	https://hardening-mediawiki/index.php/Spezial:Liste_der_Sperren
Other information	10.192.5.247
URL	https://hardening-mediawiki/index.php/Spezial:Liste_der_Sperren
Other information	10.192.5.247
URL	https://hardening-mediawiki/index.php/Spezial:Liste_der_Sperren
Other information	10.192.5.247
URL	https://hardening-mediawiki/index.php/Spezial:Liste_der_Sperren
Other information	10.192.5.247
URL	https://hardening-mediawiki/index.php/Spezial:Liste_der_Sperren
Other information	10.192.5.247
URL	https://hardening-mediawiki/index.php/Spezial:Liste_der_Sperren
Other information	10.192.5.247
URL	https://hardening-mediawiki/index.php/Spezial:Liste_der_Sperren

Other information	10.192.5.247
Solution	Remove the private IP address from the HTTP response body. For comments, use jsp/asp comment instead of HTML/javascript comment which can be seen by client browsers.
Reference	

Low (Warning) Obsolete file extended check

Description	Miscellaneous include files, backup, unused or obsolete files exist as indicated. If these files contain program source, information such as server logic or ODBC/JDBC user ID and passwords may be revealed since these file extension may not be processed by the web server.
URL	https://hardening-mediawiki/skins.Inc
URL	https://hardening-mediawiki/skins~
URL	https://hardening-mediawiki/skins.INC
URL	https://hardening-mediawiki/skins.Inc
URL	https://hardening-mediawiki/skins.java
URL	https://hardening-mediawiki/skins.INC
URL	https://hardening-mediawiki/skins.Bak
URL	https://hardening-mediawiki/skins.java
URL	https://hardening-mediawiki/skins.BAK
URL	https://hardening-mediawiki/skins.Bak
URL	https://hardening-mediawiki/index.php/Spezial:Browse/Semantisches_eStudy_Wiki~
URL	https://hardening-mediawiki/skins.BAK
URL	https://hardening-mediawiki/skins.Old
URL	https://hardening-mediawiki/index.Inc

URL	https://hardening-mediawiki/skins.Old
URL	https://hardening-mediawiki/index.php/Spezial:Browse/Semantisches_eStudy_Wiki.Inc
URL	https://hardening-mediawiki/skins.OLD
URL	https://hardening-mediawiki/index.INC
URL	https://hardening-mediawiki/index.java
URL	https://hardening-mediawiki/index.php/Spezial:Browse/Semantisches_eStudy_Wiki.INC
URL	https://hardening-mediawiki/index.php/Spezial:Browse/Semantisches_eStudy_Wiki.java
URL	https://hardening-mediawiki/skins.OLD
URL	https://hardening-mediawiki/index.Inc
URL	https://hardening-mediawiki/index.Bak
URL	https://hardening-mediawiki/index.BAK
URL	https://hardening-mediawiki/index.php/Spezial:Browse/Semantisches_eStudy_Wiki.Bak
URL	https://hardening-mediawiki/index.php/Spezial:Browse/Semantisches_eStudy_Wiki.BAK
URL	https://hardening-mediawiki/index.INC
URL	https://hardening-mediawiki/index.java
URL	https://hardening-mediawiki/index.Old
URL	https://hardening-mediawiki/index.OLD
URL	https://hardening-mediawiki/index.php/Spezial:Browse/Semantisches_eStudy_Wiki.Old
URL	https://hardening-mediawiki/index.php/Spezial:Browse/Semantisches_eStudy_Wiki.OLD
URL	https://hardening-mediawiki/index.Bak
URL	https://hardening-mediawiki/index.Inc
URL	https://hardening-mediawiki/index.BAK

URL	https://hardening-mediawiki/index.INC
URL	https://hardening-mediawiki/index.Old
URL	https://hardening-mediawiki/index.java
URL	https://hardening-mediawiki/index.OLD
URL	https://hardening-mediawiki/index.Inc
URL	https://hardening-mediawiki/index.Bak
URL	https://hardening-mediawiki/index.INC
URL	https://hardening-mediawiki/index.BAK
URL	https://hardening-mediawiki/index.java
URL	https://hardening-mediawiki/index.Old
URL	https://hardening-mediawiki/index.Bak
URL	https://hardening-mediawiki/index.OLD
URL	https://hardening-mediawiki/index.Inc?select=Stats&action=menu
URL	https://hardening-mediawiki/index.BAK
URL	https://hardening-mediawiki/index.Old
URL	https://hardening-mediawiki/index.INC?select=Stats&action=menu
URL	https://hardening-mediawiki/index.OLD
URL	https://hardening-mediawiki/index.java?select=Stats&action=menu
URL	https://hardening-mediawiki/index.BAK?select=Stats&action=menu
URL	https://hardening-mediawiki/index.Bak?select=Stats&action=menu
URL	https://hardening-mediawiki/index.Inc
URL	https://hardening-mediawiki/index.Old?select=Stats&action=menu

URL	https://hardening-mediawiki/index.INC
URL	https://hardening-mediawiki/index.OLD?select=Stats&action=menu
URL	https://hardening-mediawiki/index.java
URL	https://hardening-mediawiki/index.Inc
URL	https://hardening-mediawiki/index.Bak
URL	https://hardening-mediawiki/index.INC
URL	https://hardening-mediawiki/index.BAK
URL	https://hardening-mediawiki/index.java
URL	https://hardening-mediawiki/index.Old
URL	https://hardening-mediawiki/index.Bak
URL	https://hardening-mediawiki/index.OLD
URL	https://hardening-mediawiki/index.BAK
URL	https://hardening-mediawiki/index.Inc
URL	https://hardening-mediawiki/index.Old
URL	https://hardening-mediawiki/index.INC
URL	https://hardening-mediawiki/index.OLD
URL	https://hardening-mediawiki/index.java
URL	https://hardening-mediawiki/index.Inc
URL	https://hardening-mediawiki/index.Bak
URL	https://hardening-mediawiki/index.INC
URL	https://hardening-mediawiki/index.BAK
URL	https://hardening-mediawiki/index.java

URL	https://hardening-mediawiki/index.Old
URL	https://hardening-mediawiki/index.Bak
URL	https://hardening-mediawiki/index.OLD
URL	https://hardening-mediawiki/index.BAK
URL	https://hardening-mediawiki/images~
URL	https://hardening-mediawiki/index.Old
URL	https://hardening-mediawiki/index.OLD
URL	https://hardening-mediawiki/images.Inc
URL	https://hardening-mediawiki/index.Inc
URL	https://hardening-mediawiki/images.Inc
URL	https://hardening-mediawiki/index.INC
URL	https://hardening-mediawiki/images.INC
URL	https://hardening-mediawiki/index.java
URL	https://hardening-mediawiki/images.INC
URL	https://hardening-mediawiki/index.Bak
URL	https://hardening-mediawiki/images.java
URL	https://hardening-mediawiki/index.BAK
URL	https://hardening-mediawiki/images.java
URL	https://hardening-mediawiki/index.Old
URL	https://hardening-mediawiki/images.Bak
URL	https://hardening-mediawiki/index.OLD
URL	https://hardening-mediawiki/images.Bak

URL	https://hardening-mediawiki/images.BAK
URL	https://hardening-mediawiki/images.BAK
URL	https://hardening-mediawiki/images.Old
URL	https://hardening-mediawiki/extensions~
URL	https://hardening-mediawiki/images.Old
URL	https://hardening-mediawiki/extensions.Inc
URL	https://hardening-mediawiki/images.OLD
URL	https://hardening-mediawiki/extensions.Inc
URL	https://hardening-mediawiki/images.OLD
URL	https://hardening-mediawiki/extensions.INC
URL	https://hardening-mediawiki/extensions.java
URL	https://hardening-mediawiki/extensions.INC
URL	https://hardening-mediawiki/extensions.Bak
URL	https://hardening-mediawiki/extensions.java
URL	https://hardening-mediawiki/extensions.BAK
URL	https://hardening-mediawiki/extensions.Bak
URL	https://hardening-mediawiki/extensions.Old
URL	https://hardening-mediawiki/extensions.BAK
URL	https://hardening-mediawiki/extensions.Old
URL	https://hardening-mediawiki/index.Inc?title=Semantisches_eStudy_Wiki&action=submit
URL	https://hardening-mediawiki/extensions.OLD
URL	https://hardening-mediawiki/index.INC?title=Semantisches_eStudy_Wiki&action=submit

URL	https://hardening-mediawiki/extensions.OLD
URL	https://hardening-mediawiki/index.java?title=Semantisches_eStudy_Wiki&action=submit
URL	https://hardening-mediawiki/index.Inc?title=Semantisches_eStudy_Wiki&action=submit
URL	https://hardening-mediawiki/index.Bak?title=Semantisches_eStudy_Wiki&action=submit
URL	https://hardening-mediawiki/index.INC?title=Semantisches_eStudy_Wiki&action=submit
URL	https://hardening-mediawiki/index.BAK?title=Semantisches_eStudy_Wiki&action=submit
URL	https://hardening-mediawiki/index.Old?title=Semantisches_eStudy_Wiki&action=submit
URL	https://hardening-mediawiki/index.java?title=Semantisches_eStudy_Wiki&action=submit
URL	https://hardening-mediawiki/index.BAK?title=Semantisches_eStudy_Wiki&action=submit
URL	https://hardening-mediawiki/index.Bak?title=Semantisches_eStudy_Wiki&action=submit
URL	https://hardening-mediawiki/index.Old?title=Semantisches_eStudy_Wiki&action=submit
URL	https://hardening-mediawiki/index.OLD?title=Semantisches_eStudy_Wiki&action=submit
URL	https://hardening-mediawiki/index.Inc?title=Semantisches_eStudy_Wiki&action=history
URL	https://hardening-mediawiki/index.OLD?title=Semantisches_eStudy_Wiki&action=submit
URL	https://hardening-mediawiki/index.java?title=Semantisches_eStudy_Wiki&action=history
URL	https://hardening-mediawiki/index.INC?title=Semantisches_eStudy_Wiki&action=history
URL	https://hardening-mediawiki/index.BAK?title=Semantisches_eStudy_Wiki&action=history
URL	https://hardening-mediawiki/index.Bak?title=Semantisches_eStudy_Wiki&action=history
URL	https://hardening-mediawiki/index.OLD?title=Semantisches_eStudy_Wiki&action=history
URL	https://hardening-mediawiki/index.Old?title=Semantisches_eStudy_Wiki&action=history

Solution	Remove backup, unused or obsolete files. For include files, carefully choose the suffix to prevent information disclosure.
----------	--

Reference